WASHINGTON, D.C. – Congresswoman Loretta Sanchez (CA-47), Chair of the House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, delivered the following opening statement during today's hearing on the importance of public-private partnerships in the development of cybersecurity policy:

"Good afternoon. Before we begin, since this is my first TUTC Subcommittee Hearing as Chairwoman, I would like to share that I am extremely honored to be serving in this new role and I look forward to working with the Subcommittee Members and staff. I would like to welcome you all and thank you for joining us today to discuss cybersecurity – a high priority issue for the Department of Defense and for the security of the nation as a whole.

"Today, our witnesses will be providing us with private sector perspectives on the Department of Defense's information technology and cybersecurity activities. Cybersecurity is an issue I have been following very closely as a member of the House Armed Services Committee and as the Vice-Chair of the Homeland Security Committee. Cyber threats have only recently received the attention they deserve, particularly within the defense community.

"DoD is continually working to gain a better understanding of cybersecurity and how to best protect this nation's cyberspace. There have been many mainstream discussions in the press regarding cybersecurity, in large part because of the publicity around the hacking attacks on Google.

"However, there have been a number of high profile events against the DoD and others, including cyberattacks against Estonian and Georgian government forces, reports of intrusions into contractor networks to exfiltrate data on the F-35 Joint Strike Fighter, intrusions into the networks that control our electricity grid, and intrusions on Pentagon email networks. These are only a few instances that we know of.

"Many people are unaware that our systems, especially our defense networks, are attacked on a daily basis. In the Department of Defense, there are more than 15,000 different computer networks which are operated across 4,000 military installations around the world. We must protect these systems and ensure that information on them is only accessible to authorized personnel.

“We must not only be prepared to respond quickly and effectively to a cyberattack but we must invest in the necessary resources to protect our systems. This is why it is important that the government engage the private sector as a partner in cybersecurity, and not simply as a technology provider.

“There is a vast array of intellectual capital and expertise in the private sector that is not adequately consulted on key strategic questions, even though decisions will typically have as much of an impact on industry as it will on government. We should recognize that the private sector is very much part of the DoD family, and should be treated that way. DoD works with countless defense industries and these industries must also be held responsible for handling classified and sensitive unclassified information appropriately.

“While DoD may find it difficult to engage with industry, that is not the case for Congress, and we feel that gaining insight from the private sector is essential. We hope that the witnesses today will share their views on a broad range of topics to further inform our awareness of these issues as we work with the DoD to craft an appropriate strategy for defending and operating in cyberspace. I feel the views of our private sector witnesses will be a valuable complement to the views of the DoD.

“For example, understanding the implications of how the recent QDR addressed the issue of cyberspace, will be incredibly valuable, as would thoughts on the proposed direction for the newly established Cyber Command.

“A major focus of this subcommittee is on the science and technology programs of the DoD, so getting an outside view on the proposed research agenda would also be valuable. With a proposed increase of more than $70 million in *new* funding for computer science and security research in the S&T budget this year, I would like to better understand, from a private sector perspective, whether we are investing in the right areas. If not, where should we be investing this new funding?

“We must better protect our information networks before we experience more situations where state and non-state actors are able to infiltrate our systems and not only steal data on our weapons systems but also put lives in danger by disrupting military operations on the frontlines.

“Once again I would like to thank all of our witnesses for being here today and I look forward to hearing your testimonies. I will now yield to the Ranking Member from Florida, Mr. Miller for his opening statement. Thank you.”

# # #